

SEP-02-2005 12:35 FROM:ROBERT M. McDERMOTT 2152437525


TO:USPTO SEP 02 2005 11:12

Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005

Page 1 of 11

IN THE UNITED STATES  
PATENT AND TRADEMARK OFFICE

Appl. No. : 09/548,728  
Applicant(s) : EPSTEIN  
Filed : 13 Apr 2000  
TC/A.U. : 2131  
Examiner : REVAK, Christopher A.  
Atty. Docket : PHA 23,671

<p>CERTIFICATE OF MAILING OR TRANSMISSION</p> <p>I certify that this correspondence is being:</p> <p>[ ] deposited with the U.S. Postal Service with sufficient postage as first-class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.</p> <p>[X] transmitted by facsimile to the U.S. Patent and Trademark Office at 571-273-8300.</p> <p>On: 2 September 2005</p> <p>By: </p>
--

Title: REGISTERING COPY PROTECTED MATERIAL IN A CHECK-OUT, CHECK-IN  
SYSTEM

Mail Stop: APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Alexandria, VA 22313-1450

APPEAL UNDER 37 CFR 41.37

Sir:

This is an appeal from the decision of the Examiner dated 21 April 2005, finally  
rejecting claims 1-2, 4-5, and 11-14 of the subject application.

This paper includes (each beginning on a separate sheet):

1. Appeal Brief, with appendices; and
2. Credit card authorization in the amount of \$500.

09/06/2005 MBINAS 00000035 09548728

01 FC:1402

500.00 0P

PHA 23,671 Appeal Brief 5.421

Atty. Docket No. PHA 23,671

SEP 02 2005

SEP-02-2005 12:35 FROM:ROBERT M. MCDERMOTT 2152437525

TO:USPTO

P.2/12

Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005

Page 2 of 11

## APPEAL BRIEF

### I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to **Philips Electronics North America**.

### II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

### III. STATUS OF CLAIMS

Claims 1-14 are pending in the application.

Claims 6-10 are allowed; claim 3 is allowable if rewritten in independent form.

Claims 1-2, 4-5, and 11-14 stand rejected by the Examiner under 35 U.S.C. 102(b).

These rejected claims are the subject of this appeal.

### IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection in the Office Action dated 21 April 2005. A reply to the final rejection was filed on 5 June 2005.

### V. SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to a check-out/check-in system that provides a "one-at-a-time" or an "at-most-N-at-a-time" copy scheme to limit the number of simultaneously available copies of protected content material (page 2, lines 5-7). Such a system is used, for example, to limit the number of copies of material concurrently provided to portable devices, such as MP3 players. When a 'conforming' receiving device receives a copy of the material (check-out), the system increments a tally; when the copy of the material is removed from the receiving device (check-in),

**Appl. No. 09/548,728**  
**Appeal Brief in Response**  
**to final Office action of 21 April 2005**

**Page 3 of 11**

the system decrements the tally. The check-out/check-in system of this invention assures that the device that "checks-in" a copy of content material is the same device that "checked-out" the copy, using a secure challenge-response protocol (page 2, line 29 through page 3, line 6). Preferably, the 'challenge' is a random number that is encrypted by the check-out/check-in system, using a public key of a public-private key pair that is associated with the receiving device (page 5, lines 11-13); the 'response' from the receiving device is a decryption of the random number, using the private key that is secret to the receiving device (page 6, lines 5-8). Other security challenge-response techniques may also be used (page 5, lines 10-11).

As claimed in independent claim 1, upon which claims 2-5 depend, the invention comprises a method that includes communicating a copy of the content material to a receiving device (page 5, lines 1-2), communicating a security challenge to the receiving device when the copy of the content material is communicated to the receiving device (page 5, lines 8-11; 350 in FIG. 2), and receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device (page 6, lines 1-5; 370 in FIG. 2).

As claimed in independent claim 11, upon which claims 12-14 depend, the invention comprises a receiving device (200) that includes a memory (210) that is configured to store the content material and the corresponding security challenge (page 5, lines 17-18), and a security device (220) that is configured to erase the content material from the memory (page 6, lines 1-3), and communicate a security response to a check-out/check-in device (100), based on the security challenge that is associated with the content material (page 6, lines 3-5).

As claimed in dependent claim 13, upon which claim 14 depends, the security device (220) includes a decrypter (230) that decrypts the security challenge via a

Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005

Page 4 of 11

private key (212) of a public-private key pair that is associated with the receiving device to form the security response (page 6, lines 5-8).

#### **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 1-2, 4-5, and 11-14 stand rejected under 35 U.S.C. 102(b) over Ananda (USP 5,638,513).

#### **VII. ARGUMENT**

**Claims 1-2, 4-5, and 11-14 stand rejected  
under 35 U.S.C. 102(b) over Ananda**

##### **Claims 1-2 and 4-5**

As claimed in independent claim 1, the claimed method includes communicating a security challenge to a receiving device when the copy of the content material is communicated to the receiving device, and receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device.

Ananda teaches a software rental system that provides access to the rented software by a first computer only when a communication link is maintained between the first computer and a second, controlling computer (Ananda's abstract, lines 1-5). When the communication link is interrupted or terminated, the rented software no longer executes on the first computer (Ananda's abstract, lines 12-15). The rented software is downloaded to the first computer, with a header that includes a security program that is launched when the rented software is executed (Ananda, column 3, line 65 through column 4, line 6). The security program runs asynchronously while the rented software is running, and periodically verifies that the first computer is in communication with the central rental facility (Ananda, column 4, lines 12-20). When a communication failure is detected, the security program terminates the execution of the rented program (1016-1018 of FIG. 10A; column 16, lines 37-45).

**Appl. No. 09/548,728**  
**Appeal Brief in Response**  
**to final Office action of 21 April 2005**

**Page 5 of 11**

Ananda does not teach receiving a security response, based on a security challenge, from the receiving device when the copy of the content material is removed from the receiving device.

The Office action notes that the applicant has defined 'removal' of the content material to include terminating access to the material; the applicant concurs with this definition of 'removal'. Using this definition, the Office action asserts that Ananda's termination of access to the rented software constitutes removal of the rented software. The applicant notes, however, that when Ananda terminates access, Ananda merely informs the user that access has been terminated.

The Office action asserts that Ananda teaches a security response based on a security challenge at column 9, line 66 through column 10, line 10. However, this passage recites that the security manager on the user's computer verifies communication with the rental agency. Ananda is silent with regard to a challenge-response protocol. As the terms 'challenge' and 'response' are conventionally used, the computer that is performing the verification issues the 'challenge', and performs the verification based on a received 'response'. Thus, the applicant respectfully maintains that Ananda's user computer communicates the security 'challenge' and does not communicate the security 'response', as the term security response is conventionally used, and as defined and used in the applicant's specification. Further, Ananda specifically teaches that the security program on the user's computer issues a transfer time request to the rental facility, then waits up to 30 seconds for a response; if the response is not received after 30 seconds, the security program concludes that communications have ceased, and terminates the rented software (Ananda, column 16, lines 27-40). The applicant respectfully maintains that the transmission of a request and taking action based on an improper response or the lack of response corresponds to a conventional definition of a challenge (request) – response protocol, with Ananda's security program on the user's computer corresponding to the issuer of the challenge. With specific regard to claim 1, the receiving device is the device that receives the content material, i.e. Ananda's user's

Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005

Page 6 of 11

computer; Ananda does not teach receiving a secure response *from* the user's computer based on a security challenge that is transmitted *to* the user's computer.

Further, assuming in argument that Ananda's user's computer can be considered the transmitter of a security response, the applicant notes that it is the *absence* of communication between the user's computer and the rental facility for at least 30 seconds that causes the termination of access to the rented software, and thus a security response cannot be *received* from the user's computer when this access is terminated, because this is when there are *no* communications between the user's computer and the rental facility.

MPEP 2131 clearly states:

"A claim is anticipated only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The *identical invention* must be shown in as *complete detail* as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Because Ananda fails to teach each of the elements of claim 1, upon which claims 2-5 depend, the applicant respectfully maintains that the rejection of claims 1-2 and 4-5 under 35 U.S.C. 102(b) over Ananda is unfounded, per MPEP 2131.

#### Claims 11-14

As claimed in independent claim 11 the invention comprises a receiving device that includes a memory that is configured to store content material and a corresponding security challenge, and a security device that is configured to erase the content material from the memory, and communicate a security response to a check-out/check-in device, based on the security challenge that is associated with the content material.

The Office action asserts that Ananda teaches a receiving device that receives and stores content material and a corresponding security challenge, but fails to support this assertion. As noted above, Ananda is silent with regard to the terms 'security challenge' and 'security response', and a conventional interpretation of Ananda's teachings does not support a conclusion that Ananda's receiving device

**Appl. No. 09/548,728**  
**Appeal Brief in Response**  
**to final Office action of 21 April 2005**

**Page 7 of 11**

receives a security challenge associated with the content material, or that Ananda's receiving device stores such a challenge.

The Office action also asserts that Ananda teaches that the receiving device erases the content material and communicates a security response based on the security challenge. The applicant maintains that Ananda does not teach receiving a security challenge associated with the content material, and thus cannot be said to teach communicating a security response based on such a challenge.

Because Ananda fails to teach each of the elements of claim 11, upon which claims 12-14 depend, the applicant respectfully maintains that the rejection of claims 11-14 under 35 U.S.C. 102(b) over Ananda is unfounded, per MPEP 2131, cited above.

#### **Claims 13-14**

Claim 13, upon which claim 14 depends, claims the receiving device of claim 11, wherein the security device includes a decryptor that decrypts the security challenge to form the security response that is communicated to a check-in/check-out device.

Ananda's decryptor decrypts a password that is received from the rental facility, and compares it to a password stored in its memory to determine whether to allow continued access to the rented software (column 15, lines 35-45). The applicant respectfully maintains that this password is a security response, and not a security challenge.

Assuming in argument that Ananda's password message from the rental facility can be said to correspond to the applicant's claimed security challenge, Ananda's decryptor does not form a security response that is transmitted to the check-in/check-out device (rental facility), as specifically claimed in claim 13.

Because Ananda fails to teach each of the elements of claim 13, upon which claim 14 depends, the applicant respectfully maintains that the rejection of claims 13 and 14 under 35 U.S.C. 102(b) over Ananda is unfounded, per MPEP 2131, cited above.

Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005

Page 8 of 11

### CONCLUSIONS

Because Ananda does not teach communicating a security challenge to a receiving device when the copy of the content material is communicated to the receiving device, and receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device, as specifically claimed in claim 1, the applicant respectfully requests that the Examiner's rejection of claims 1-5 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Because Ananda does not teach a receiving device that includes a memory that is configured to store content material and a corresponding security challenge, and does not teach a security device that is configured to erase the content material from the memory, and communicate a security response based on the security challenge that is associated with the content material, as specifically claimed in claim 11, the applicant respectfully requests that the Examiner's rejection of claims 11-14 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Because Ananda does not teach a decrypter that decrypts a security challenge to form a security response that is communicated to a check-in/check-out device, as specifically claimed in claim 13, the applicant respectfully requests that the Examiner's rejection of claims 13-14 under 35 U.S.C. 102(b) be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,



Robert M. McDermott, Attorney  
Registration Number 41,508  
804-493-0707



**Appl. No. 09/548,728  
Appeal Brief in Response  
to final Office action of 21 April 2005**

**Page 9 of 11**

### **CLAIMS APPENDIX**

1. A method for limiting simultaneous copies of content material, comprising:  
communicating a copy of the content material to a receiving device,  
communicating a security challenge to the receiving device when the copy of the content material is communicated to the receiving device, and  
receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device.
2. The method of claim 1, further including  
verifying a certification of the receiving device before communicating the copy of the content material to the receiving device.
3. (Allowable)
4. The method of claim 1, further including:  
generating a random number, and  
encrypting the random number via a public key of a public-private key pair that is associated with the receiving device to form the security challenge, and  
wherein  
the security response includes the random number.
5. The method of claim 4, further including  
verifying a certification of the receiving device before communicating the copy of the content material to the receiving device, and  
wherein  
the certification of the receiving device includes a public key of the public-private key pair of the receiving device.
- 6-10 (Allowed)

**Appl. No. 09/548,728  
Appeal Brief In Response  
to final Office action of 21 April 2005**

**Page 10 of 11**

11. A receiving device that receives content material and a corresponding security challenge from a check-out/check-in device, comprising:

a memory that is configured to store the content material and the corresponding security challenge, and

a security device that is configured to:  
erase the content material from the memory, and  
communicate a security response to the check-out/check-in device,  
based on the security challenge that is associated with the content material.

12. The receiving device of claim 11, wherein

the security device is further configured to communicate a certification of the receiving device to the check-out/check-in device to enable the check-out/check-in device to provide the content material to the receiving device.

13. The receiving device of claim 11, wherein

the security device includes:  
a decrypter that decrypts the security challenge via a private key of a public-private key pair that is associated with the receiving device to form the security response.

14. The receiving device of claim 13, wherein

the security device is further configured to communicate a certification of the receiving device to the check-out/check-in device to enable the check-out/check-in device to provide the content material to the receiving device, and

the certification of the receiving device includes a public key of the public-private key pair of the receiving device.

**Appl. No. 09/548,728  
Appeal Brief In Response  
to final Office action of 21 April 2005**

**Page 11 of 11**

### **EVIDENCE APPENDIX**

No evidence has been submitted that is relied upon by the appellant in this appeal.

### **RELATED PROCEEDINGS APPENDIX**

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.